UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,454	08/14/2001	Liqun Chen	B-4278PCT	9593

22879 7590 10/15/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
10/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	Application No.	Applicant(s)	
	09/913,454	CHEN ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *44-53 and 57-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *44-53 and 57-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to the communication dated 8/16/07 with the amendments to claims 52, 57 and 59; the addition of claims 65-67 and the cancellation of claims 54-56.

2. Claims 44-53 and 57-67 are pending.

Response to Arguments

3. Applicant's arguments filed 8/16/07 have been fully considered but they are not persuasive.

The Applicant argues that Probst compares the encrypted configuration data against the actual configuration data, not the stored module configuration against the actual module configuration as in claim 44. The Examiner respectfully disagrees, the encrypted configuration data is the data stored on a storage device of the computer system and is used for verifying the configuration (Probst: col. 3, lines 43-45), as such, it reads on the stored module configuration of claim 44.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., Probst's processor 31 as "trusted device" is not tamper-resistant or tamper-detecting as recited in claim 44) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are

not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's arguments, the recitation "the trusted device" of claim 44 is "adapted to respond to a user in a trusted manner" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

The Applicant argues that Probst does not disclose inhibiting the function of the computer. The Examiner respectfully submits that Probst teaches if a mismatch occurs, (as a result of the comparison) the entire system is disable (i.e. inhibiting function of the computer) (Probst: col. 4, lines 24-25; col. 7, lines 49-53).

The Applicant argues that the concept of determining the stored module configuration by using a cryptographic identification process with a cryptographic identity can be implemented for determining actual module configuration. The Examiner respectfully submits that it is well-known in the data communication world that encrypting is used to protect data for security reason that is disclosed by Probst (Fig. 1). For that same reason, the actual configuration data can be protected by implementing that same concept that is used for the stored encrypted configuration data as taught by Probst. The previous office action asserted Fig. 2, elements 7-11 to illustrate how the

stored encrypted module configuration is derived by inversing the encryption process, it is well-understood that one cannot decrypt data that is not encrypted as submitted in the Remarks.

The Applicant argues that Probst teaches away when "the actual configuration data is stored in unencrypted form". The Examiner respectfully disagrees, Probst discloses alternatively the actual configuration data is encoded by means of the identifier (col. 4, lines 19-23). As such, it still performs a cryptographic identification process for modules with a cryptographic identity.

Claim Rejections - 35 USC § 112

4. The rejections under 35 U.S.C 112 have been withdrawn based on the filed amendments.

Claim Objections

5. Claim 57 is objected to because of the following informalities: the limitation "the step of inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration" is listed twice.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 44-47, 50 and 52-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Probst (5,982,899) in view of Selitrennikoff et al. (6,209,089).

a) As to claim 44, Probst discloses a method of protecting from modification computer apparatus (see Probst: col. 3, lines 1-3) comprising a plurality of functional modules, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, the method comprising storing a module configuration of the computer apparatus (see Probst: col. 3, lines 8-30); the trusted device performing a cryptographic identification process for modules with a cryptographic identity to identify them and thereby determine an actual module configuration (i.e. the actual module configuration is read and later compared with the stored data, see Probst: col. 5, lines 51-53. Probst discloses a cryptographic identification process with a cryptographic identity to determine the stored module configuration (see Probst: Fig. 2, elements 7-11). That concept can be implemented for determining actual module configuration for modules by a cryptographic identification process with a cryptographic identity); the trusted device comparing the actual module configuration against the stored module configuration (see Probst: col. 4, lines 11-14); and the trusted device inhibiting function of the computer apparatus while the actual module configuration does not satisfactorily match the stored module configuration (see Probst: col. 4, lines 24-25).

Probst discloses an identifier for the entire computer system (see Probst: col. 3, lines 62-63), however Probst is silent on a module configuration providing an identification of each functional module in the computer apparatus.

Selitrennikoff is relied on for the teaching of a module configuration providing an identification of each functional module in the computer apparatus (see Selitrennikoff: col. 13, lines 20-24; Fig. 3, element 40).

It would be obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a module configuration providing an identification of each functional module in the computer apparatus in the system of Probst, as Selitrennikoff teaches, so as to uniquely distinguish the functional modules from one another.

b) As to claim 45, the combination of Probst and Selitrennikoff discloses the method of claim 44, wherein the stored module configuration is held separately from the computing apparatus (i.e. over the network, see Probst: col. 3, lines 53-54).

c) As to claim 46, the combination of Probst and Selitrennikoff discloses the method of claim 44, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process (see Probst: Fig. 2, elements 7-11).

d) As to claim 47, the combination of Probst and Selitrennikoff discloses the method of claim 44, wherein the trusted device is adapted to communicate securely with the stored module configuration (i.e. Probst discloses the validation and authentication process with the use of public/private key, see Probst: Figs 1 and 2).

e) As to claim 50, please see the addressed claim 44 above.

f) As to claim 52, this claim is directed to a hardware implementation of the method of claim 44 and is rejected by a similar rationale applied against claim 44 above.

g) As to claim 53, this claim is directed to a hardware implementation of the method of claims 45-46 and is rejected by a similar rationale applied against claim 45-46 above.

8. Claims 48-49, 57-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Probst (5,982,899) in view of in view of Selitrennikoff et al. (6,209,089) and further in view of Herzi et al. (6,353,885).

a) As to claims 48 and 49, the combination of Probst and Selitrennikoff discloses the method of claim 47, however it is silent on the capability of the stored module configuration is stored in a security token and wherein the security token is a smart card.

Herzi is relied on for the teaching of having the stored module configuration is stored in a security token and wherein the security token is a smart card (i.e. stored module configuration contains BIOS level settings is stored in a smart card, see Herzi: col. 3, lines 54-57; col. 3, lines 5-13).

It would be obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a security token adapted to hold a stored module configuration of modules in a computer apparatus in the system of Probst and Selitrennikoff, as Herzi teaches so as to flexibly provide a computer configuration in a multi-user computer system environment (see Herzi: col. 2, lines 3-5).

b) As to claim 57, Probst discloses a method of protecting from modification computer apparatus (see Probst: col. 3, lines 1-3) comprising a plurality of functional modules, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, the method comprising storing a module configuration of the computer apparatus (see Probst: col. 3, lines 8-30); checking an actual module configuration against the stored module configuration (see Probst: col. 4, lines 11-14); and inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration (see Probst: col. 4, lines 24-25); wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner (i.e. trusted manner in a sense that it inhibits function of the computer apparatus if the actual configuration does not match the stored configuration, Probst: Fig. 4) and the trusted device is adapted to perform the step of inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration (Probst: col. 4, lines 24-25).

Probst discloses an identifier for the entire computer system (see Probst: col. 3, lines 62-63), however Probst is silent on a module configuration providing an identification of each functional module in the computer apparatus.

Selitrennikoff is relied on for the teaching of a module configuration providing an identification of each functional module in the computer apparatus (see Selitrennikoff: col. 13, lines 20-24; Fig. 3, element 40).

It would be obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a module configuration providing an identification of each functional module in the computer apparatus in the system of Probst, as Selitrennikoff teaches, so as to uniquely distinguish the functional modules from one another.

The combination of Probst and Selitrennikoff is silent on the capability of storing a module configuration of the computer apparatus on a security token removably attachable to the computer apparatus.

Herzi is relied on for the teaching of storing a module configuration of the computer apparatus on a security token removably attachable to the computer apparatus (i.e. stored module configuration contains BIOS level settings is stored in a smart card, see Herzi: col. 3, lines 54-57; col. 3, lines 5-13).

It would be obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a security token adapted to hold a stored module configuration of modules in a computer apparatus in the system of Probst and Selitrennikoff, as Herzi teaches so as to flexibly provide a computer configuration in a multi-user computer system environment (see Herzi: col. 2, lines 3-5).

c) As to claim 58, the combination of Probst and Selitrennikoff discloses the method of claim 57, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process (see Probst: Fig. 2, elements 7-11).

d) As to claim 59, please see the addressed claim 57 above.

e) As to claim 60, the combination of Probst, Selitrennikoff and Herzi discloses the method of claim 59, wherein the trusted device is adapted to communicate securely with the stored module configuration (i.e. Probst discloses the validation and authentication process with the use of public/private key, see Probst: Figs 1 and 2).

f) As to claims 61-63, please see the addressed claim 57 above.

9. Claims 51 and 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Probst (5,982,899) in view of Selitrennikoff et al. (6,209,089) in view of Herzi et al. (6,353,885) and further in view of Muftic (5,943,423).

Probst discloses the module configuration is held by a remote module validation authority, however the combination of Probst, Selitrennikoff and Herzi is silent on the capability of the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.

Muftic is relied on for the teaching of a service allowing a replacement security token to be provided if a security token is lost or stolen (col. 6, lines 50-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of replacing lost or stolen security token as Muftic teaches in the system of Probst, Selitrennikoff and Herzi so as not to disrupt the smart card services.

10. Claims 65-67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Probst (5,982,899) in view of Selitrennikoff et al. (6,209,089) in view of Micali (5,499,296).

The combination of Probst and Selitrennikoff discloses the method of claim 44, however it is silent of the capability of having the trusted device is a tamper-resistant or a tamper-detecting device. Micali is relied on for the teaching of having the trusted device is a tamper-resistant or a tamper-detecting device (i.e. a secure device (e.g. a computer) has an encryptor in the tamper-proof area of the secure device, Micali: col. 4, lines 21-33, 60-62). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the trusted device is a tamper-resistant or a tamper-detecting device in the system of Probst and Selitrennikoff so as to maintain security of computing element).

Conclusion

11. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
10/10/07

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER